(12) UK Patent Application (19) GB (11) 2 204 971 (13) A

(43) Application published 23 Nov 1988

(21) Application No 8711741

(22) Date of filing 19 May 1987

(51) INT CL⁴
G06F 12/14 12/16

(52) Domestic classification (Edition J):
G4A AP

(56) Documents cited
GB A 2177528 GB A 2173623 GB A 2167588
GB A 2154344 GB A 2148075 EP A 0191162
WO A 85/03785 WO A 85/02696

(58) Field of search
G4A
Selected US specifications from IPC sub-class
G06F

(71) Applicant
General Electric Company Plc

(Incorporated in United Kingdom)

1 Stanhope Gate, London

(72) Inventor
Christopher John Stanford

(74) Agent and/or Address for Service
R K Tolfree
GEC Plc, Central Patent Dept, Marconi Research Centre, West Hanningfield Road, Great Baddow, Chelmsford, Essex

(54) Transportable security system

(57) In order to overcome the problem of security of data held within a program, an electronic token (3) of the type including on-board processing and memory is provided with either authentication and password software or a partially complete program, and arranged for interaction with a host computer (1) via a read/write unit (2) so that the computer will not function in a chosen manner without the presence of the token. When the token contains a partially complete program the remainder of the program is held within the computer so that both elements must be present before the program will run.

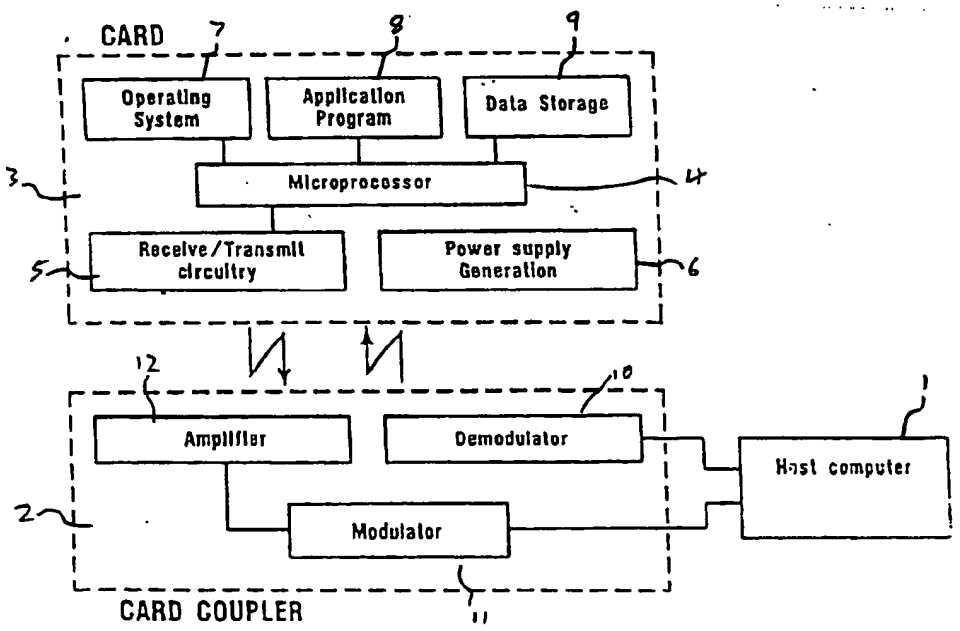

FIGURE 1

GB 2 204 971 A

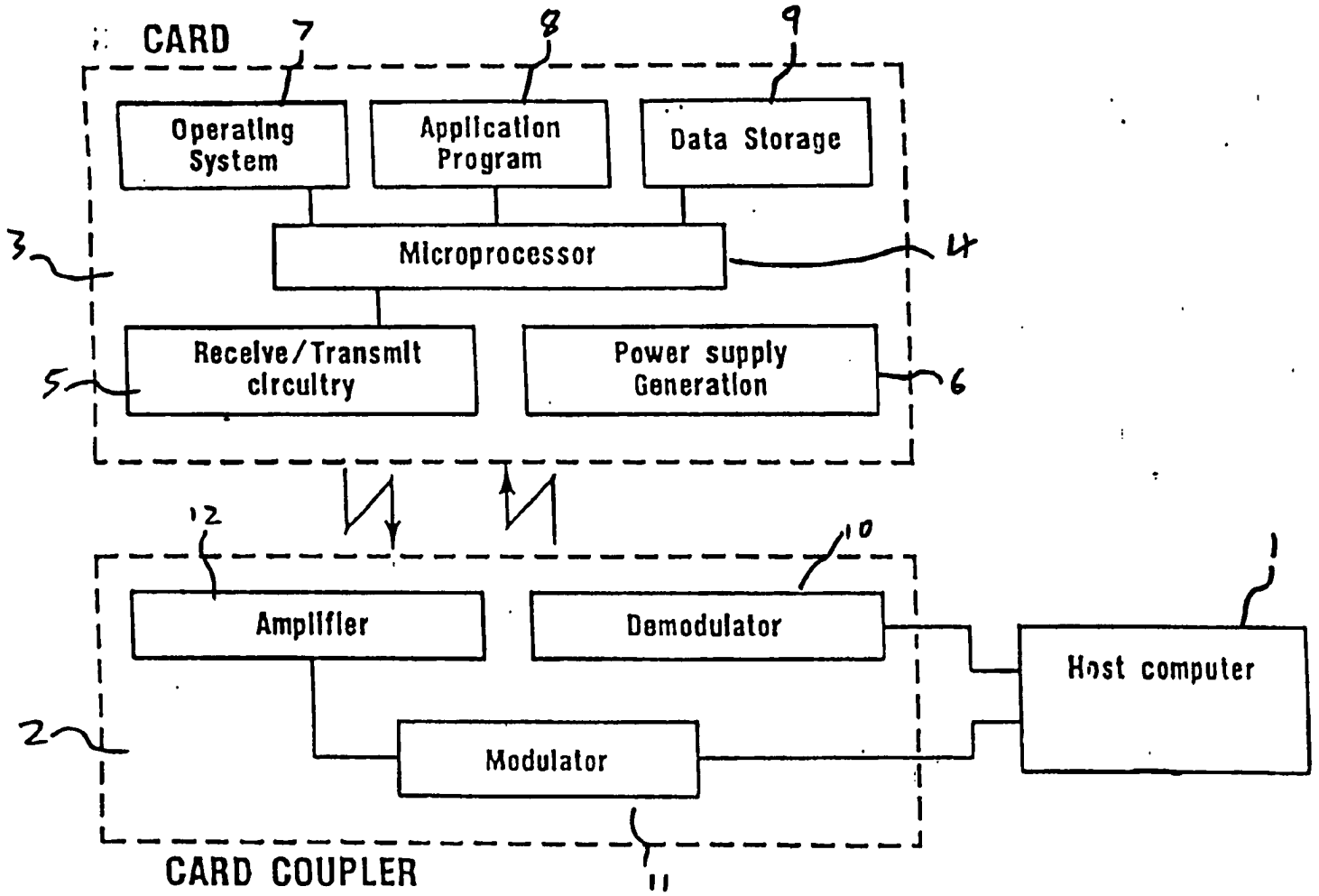

FIGURE 1

2204971

I/7356/JM

Transportable Security System

This invention relates to a transportable security system, particularly to a transportable system for the security of computer programs or for restricting access to a computer.

It should be noted that by the term 'computer' in the following specification is meant any system which includes a degree of processing or intelligence within it.

Current methods to improve the security of data or programs contained within a computer system often involve the provision of passwords or codes which must be typed in by a user before he is allowed to view or use the data. Such systems are however suspect since a person with sufficient knowledge and determination can generally 'break in' to the program within the computer to ascertain the codes or passwords required.

According to the present invention in a first aspect there is provided a security system comprising a computer; an electronic token comprising processing means, memory means and input/ output means; and means for inductively coupling the token with the computer, wherein the token and computer are each provided with a partial program which cooperate in use to provide a unitary program essential to the operation of the computer.

A plurality of tokens may be provided, each token being assigned to a particular user or class of users and including a partial program allowing its user access only to information he is authorised to access.

In use, the system may be arranged such that a computer will not function in a particular way unless one unique token is placed within operative coupling range of the computer. The token may then identify itself to the computer and a program will be allowed to run. The token could be provided with authentification and/or verification programs such that when a user enters his unique passwords or code numbers these will only be verified if the token is operatively present. The invention thus provides a far more secure system than was previously available.

Advantageously, the electronic token and its associated inductively coupled read/write unit will be of a type disclosed in the applicants published United Kingdom patent application no. GB2173623A, which is incorporated herein by reference.

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawing, which shows in block form elements of the electronic token and coupler which may be used in embodiments of the present invention.

Referring to the Figure 1 a host computer 1 is

inductively coupled by means of coupler 2 to an electronic token, shown here as Card 3. Coupling between the card and coupler is achieved inductively by means of modulated fields, as is described in the aforementioned British patent application no. GB2173623A. The Card 3 comprises a micro-processor 4 of any convenient type, a Receive/ Transmit circuit 5 and power supply means 6 which may either be an onboard battery or, more preferably, means for tapping off power which is inductively coupled from the coupler 2. The card also includes a memory region which is divided into three areas; an operating system area 7, applications program area 8 and data storage area 9.

The coupler 2 comprises a demodulator 10 and modulator 11 for processing modulated signals received or transmitted after amplification by an amplifier 12. Unmodulated signals, either after demodulation or before modulation are fed by a suitable connection to chosen address lines of the host computer 1.

In use, the card is placed with its inductive coupling coils in contact with or in a position where it will operatively couple with the coils of the coupler 2 so that, in effect, the card forms part of the computer system and signals may be transferred at will between the card and computer. By providing suitable programs in the application program area 8 of the card, by well known

programming methods, the card may be used as a security measure in any of the following ways, which are merely shown as non-limiting examples.

Firstly the card will identify itself uniquely to the system and any card not bearing the correct code within it will not be accepted and will not allow a program to run on the computer. The card can then be used to verify the identity of the user of the computer by comparing an entered PIN (Personal Identification Number) or password with a value stored in the card. Alternatively or additionally, characteristics unique to the user can be compared by means of the characteristics of a digitised signature in the card, characteristics of a voice in the card, or any other biometric characteristics such as finger prints, retina patterns, hand geometry, vein patterns etc. The card holder may be allowed to change PIN or passwords to a new value once his identity has been verified.

Apparatus of the present invention may be used to authenticate, validate, encrypt or decrypt any messages or files recieved, sent from or stored within the associated computer.

Secret keys or lists of keys to be used in authentication, encryption and decryption algorithms may be held within the token or card, and software may be included such that if one key is felt compromised then a

new key can be called into play from the cards internal memory, i.e. the processing capability of the token can be used to look for a key search which may be going on when a non-authorised person is trying to use the computer, having obtained the card. Since the card itself can hold any number of keys, within its memory capacity, then a new key does not have to be transmited to the card and new keys could be brought into play automatically dependent upon factors such as date, site of computer, time and history of use, etc. Additionally if the card detects that a person is attempting to break or illegally access the verification codes the card may be programed to erase the data or programs stored within it. This 'self destruct' feature may be initiated as a result of a number of successive threats, or perhaps be dependent upon the frequency of threats.

A multi-tier system of authorisation can be embedded within the card such that the user has to go through a number of procedures before he is allowed full access. These may be in a prescribed series or perhaps a few of them may be randomly selected by the card.

Programs may be incuded such that the card can cumulatively store details of its use, each time it has been used.

One particularly advantageous use of the card is for the card to have stored within it a portion of a program,

the remaining portion of which is stored within the computers memory. A user will then not be able to use the full program unless the card is present and operating. Furthermore, if the structure of the program is organised such that those parts carried on the card are executed entirely within the card then there is no need for the computer ever to have the complete program loaded into it and the security is greatly increased. Alternatively however that partial program could be down loaded into the computer upon start up.

It is seen that if the card or token is provided in a conventional portable form, perhaps as a credit card size token made generally from plastics material, then each user of a computer system can be provided with his own unique card which allows him to view or use only those parts of the data or program code within the computer for which he is authorised. It is also a convenient way to store and transport data for use at different terminals or different computers in different environments.

Tokens and couplers of the type described in patent application no. 2173623 may be implemented in association with small personal computers to provide a convenient security procedure and system.

CLAIMS

1. A security system comprising a computer; an electronic token comprising processing means, memory means and input/output means; and means for inductively coupling the token with the computer, wherein the token and computer are each provided with a partial program which cooperate in use to provide a unitary program essential to the operation of the computer.

2. A security system as claimed in claim 1 and including a plurality of tokens, each token being assigned to a particular user or class of users and including a partial program allowing its user access only to information he is authorised to access.

3. A security system substantially as hereinbefore described with reference to, and as illustrated by, the accompanying drawings.

Published 1988 at The Patent Office, State House, 66/71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office, Sales Branch, St Mary Cray, Orpington, Kent BR5 3RD. Printed by Multiplex techniques ltd, St Mary Cray, Kent. Con. 1/87.